IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Jesus Angel de GREGORIO RODRIGUEZ, et al. Atty. Ref.: 4020-3

Serial No. 10/510,498 TC/A.U.: 2617

Filed: October 7, 2004 Examiner: Sayed T. ZEWARI

Confirmation No.: 1556

For: SYSTEM, APPARATUS AND METHOD FOR SIM-BASED AUTHENTICATION AND ENCRYPTION IN WIRELESS LOCAL AREA NETWORK ACCESS

* *

December 22, 2009 (Tuesday)

MAIL STOP AF
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Due to the inclement weather and the closing of the Federal Government on Monday, December 21, 2009, this response is being filed on the next business day. In the Office Action dated August 20, 2009 ("Office Action"), Examiner rejects pending claims 1-25 under 35 U.S.C. § 103(a) based on various combinations of US Publication 2002/0012433 to Haverinen et al ("Haverinen"), U.S. Publication No. 2002/0009199 to Ala-Laurila et al ("Ala-Laurila"), US Patent 7,043,633 to Fink et al ("Fink"), and US Patent 6,854,014 to Amin et al ("Amin"). All rejections are clearly erroneous.

The present disclosure generally describes a telecommunication system for allowing a SIM-based authentication to users of a wireless local area network (WLAN) who are subscribers of a public land mobile network (PLMN). Fig. 1 (reproduced below) illustrates a general scenario where subscribers of a PLMN (such as GSM/GPRS/UMTS), and other local non-mobile users, access a WLAN. *See paragraph [0046] of the disclosure as originally submitted.*

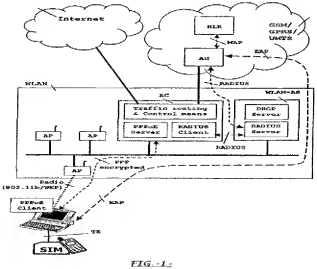


FIG. 1

In an embodiment, the Terminal Equipment (TE), which is an example of a wireless terminal, is equipped with the necessary hardware and software to interface the user's SIM card and to send and receive the required signaling information according to the Authentication and Key Agreement (AKA) protocol as well as to implement a Point-to-Point Protocol over Ethernet (PPPoE) protocol. *See paragraph [0047].*

In a non-limiting aspect, TE initially accesses the WLAN through an Access Point (AP). The Access Controller (AC), which is interposed between the AP and the PLMN, is then discovered. Afterwards, a challenge-response authentication procedure is carried out between the PLMN and the TE through the AC. The challenge-response submissions between the TE and the AC are carried on top of the PPPoE protocol as indicated by a short dash arrow between the TE and AC in Fig. 1. The IP connectivity for the TE, which includes the IP address assignment to the TE, is provided after the user is validly authenticated, that is, after the challenge-response authentication takes place.

This is reflected in independent claim 1, which recites "(c) carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, the wireless terminal provided with a SIM card and adapted for reading data thereof; wherein the challenge-response authentication submissions in step (c) takes place before having provided an IP connectivity to the user, and are carried ... on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller." As recited, the authentication procedure submissions between the TE and the Access Controller are carried out on top of the PPPoE protocol.

IP protocol enters the picture after the TE is authenticated. Claim 1 further recites "(d) offering the IP connectivity to the user at the wireless terminal, by sending an assigned IP address and other network configuration parameters, once said user has been validly authenticated by the public land mobile network." As recited, before any type of IP connectivity is provided to the TE, the TE is validly authenticated. Note that part of providing the IP connectivity is sending to the TE, the IP address assigned to the TE. That is to say, IP connectivity, including the IP address, is provided to the TE "once user has been validly authenticated."

Examiner rejects claim 1 based on a combination of Haverinen and Ala-Laurila. Examiner admits that Haverinen does not teach or suggest allocating an IP address after having authenticated the subscriber. Indeed, it was demonstrated Haverinen teaches directly the opposite – i.e., Haverinen teaches providing IP connectivity and then carrying out the authentication process over IP protocol. *See Pre-Appeal Brief Request for Review dated September 11, 2008.*

Examiner incorrectly alleges that paragraph [0020] of Ala-Laurila et al. corrects Haverinen's deficiency. *See Office Action, p.5.* Paragraph [0020] is part of Ala-Laurila that describes Fig. 1 (reproduced below).

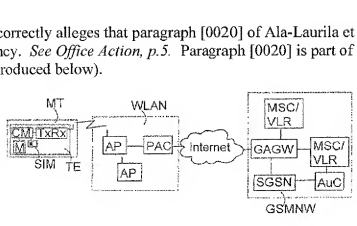
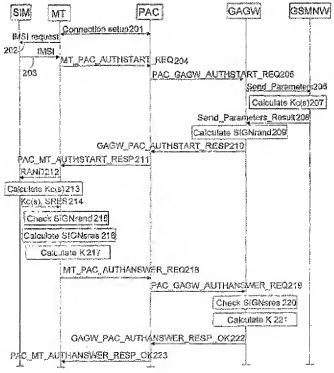


Fig. 1 illustrates a telecommunication system comprising a wireless local area network (WLAN) and a public land mobile network such as a GSM network (GSMNW). As seen, the mobile terminal MT accesses Internet services of GSMNW through the WLAN, and in particular through the Public Access Controller (PAC), which is an entity that controls access to Internet services. Paragraph [0020] actually states "In accordance with a preferred embodiment it allocates an IP address to the terminal MT and allows a connection to be established to the internet only if the terminal MT can be authenticated." Apparently, Examiner reads the phrase "only if the terminal MT can be authenticated" to apply to the entirety of "allocates an IP address to the terminal MT and allows a connection to be established to the internet." This is a misread. When properly read, the phrase "only if the terminal MT can be authenticated" applies only to "allows a connection to be established to the internet."

In Ala-Laurila, IP address allocation to the MT takes place regardless whether the MT is ultimately authenticated or not. Ala-Laurila repeatedly states that the connection between the MT, PAC, and GAGW are IP based connections. As examples, Ala-Laurila states "The interfaces between the terminal MT and the controller PAC and between the PAC and the GAGW are IP-based in accordance with a preferred embodiment of the invention" and "From now on it is assumed that the IP is used, in which case the MT, the PAC and the GAGW are identified using the IP addresses thereof." *Emphasis added; see [0023];* "The data transmission between the terminal MT and the access controller PAC may utilize messages based on an IKE (Internet Key Exchange) protocol." *See [0044].* In fact, IP connectivity between the MT and the PAC is necessary in order for the MT to be authenticated to the GSMNW in the first place.

Ala-Laurila also describes a specific process for authenticating the MT to the GSMNW in Fig. 2. Indeed, Ala-Laurila describes Fig. 2 as showing "essential functions" for authenticating the terminal MT. *See [0024]* For convenience, Fig. 2 is reproduced.



In paragraph [0024], Ala-Laurila states "The authentication process of the terminal MT is typically triggered when the MT starts setting up a connection 201 (Connection setup) with the WLAN network WLAN. Then the MT is provided with an IP address through a DHCP server

(Dynamic Host Configuration Protocol)." *Emphasis added.* The MT having been assigned the IP address submits authentication requests (e.g., MT_PAC_AUTHSTART_REQ 204) to the PAC and receives responses (e.g., PAC_MT_AUTHSTART_RESP 211) from the PAC over the IP protocol. If the authentication is ultimately not successful, the MT is simply denied services after step 223. *See [0043].*

Note the connection 201, in which the MT is assigned the IP address, occurs before any authentication message is exchanged between the MT and GAGW. In other words, MT is assigned an IP address prior to having been authenticated to the GSMNW. This is a clear indication that regardless of whether or not the MT is authenticated to access the Internet, it is assigned the IP address and the assignment occurs prior to authentication. The IP connectivity is provided so that MT, PAC, and the GAGW can exchange authentication requests and responses via the IP protocol.

The scenario illustrated in Fig. 2 is entirely dimetrically opposed to Examiner's assertion. For the Examiner's assertion to be true, it must be that the IP address for the MT is provided either in the PAC_MT_AUTHANSWER_RESP 223 sent from the PAC to the MT or immediately afterwards. However, Ala-Laurila is completely silent in this regard.

The only specific mention of the IP address assignment occurring is when the MT initially connects to the PAC in step 201 before the MT is authenticated. In short, Ala-Laurila stands for the proposition that IP connectivity is first provided to the MT, and then the authentication messages between the MT and the PAC are carried over the IP protocol. If the MT is authenticated, WLAN allows the MT to access the Internet. If not, access is denied. Thus, contrary to Examiner's assertion, Ala-Laurila does not teach or suggest allocating an IP address after having authenticated the subscriber.

Since Ala-Laurila does not teach or suggest this feature and Haverinen is also deficient, the combination of Haverinen and Ala-Laurila cannot teach or suggest this feature. Indeed, both Haverinen and Ala-Laurila teach directly the opposite. That is, both teach away. *See KSR v. Teleflex, 550 US___, 127 S.CT. 1727 (2007) ("When the prior art teaches away from combining certain know elements, discovery of successful means of combining them is more likely to be non-obvious.").* Therefore, claim 1 is not obvious over Haverinen and Ala-Laurila.

Claim 1 also recites that the challenge-response authentication submission are carried "on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller and on an authentication protocol residing at an application layer between the public land mobile network and the Access Controller." This feature is also missing from Haverinen.

Examiner states that Haverinen discloses this feature in paragraph [0343]. *See Office Action, p. 5.* Paragraph [0343] is properly understood in the context of paragraphs [0342]-[0346], in which Haverinen discloses an authentication procedure being carried out with an Extensible Authentication Protocol (EAP), which is a type of Point-to-Point Protocol (PPP), so that authentication data are exchanged between the MT and the public land mobile network (HAAA) via the PAC.

Here, the PAC does not know details of the authentication. The EAP protocol is used for exchanging authentication data between the MT and the PAC, and an EAP over RADIUS protocol is used for exchanging authentication data between the PAC and the public land mobile network (HAAA).

In contrast to Haverinen, in claim 1, the authentication submissions are carried out on top of the Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller, and on an authentication protocol residing at application layer between the public

land mobile network and the Access Controller. PPPoE is not EAP. Further, there is no suggestion in Haverinen that a challenge-response authentication is carried on top of the PPPoE. In Fig. 16 and corresponding paragraphs, there is no mention of IP connectivity occurring either before or after authentication.

For the stated reasons and others, the rejection of independent claim 1 based on Haverinen and Ala-Laurila is clearly erroneous. Independent claim 15 recites, "the Access Controller comprising ... a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the wireless terminal over a PPPoE protocol, the PPPoE server being arranged for tunneling a challenge-response authentication procedure" and "wherein the Access Controller is configured to send an assigned IP address and other network configuration parameters to the wireless terminal to provide IP connectivity after the challenge-response authentication procedure is successfully carried out between the wireless terminal and the public land mobile network in the telecommunication system." Independent claim 24 recites, "wherein an Extensible Authentication Protocol is carried on top of a Point-to-Point layer 2 protocol" and "wherein the wireless terminal is configured to receive an IP address after successfully carrying out the challenge-response authentication procedure, the IP address being usable to gain IP connectivity." For similar reasons explained for claim 1, the rejections of independent claims 15 and 24 are clearly erroneous.

Claims 2-5, 7-13, 16-22, and 25 depend from independent claims 1 and 15. Due to at least the dependencies thereon, rejections of these dependent claims are clearly erroneous. The rejections of claims 6, 14, and 23 are clearly erroneous since none of the cited secondary references Fink and Amin correct the above-noted deficiencies of Haverinen and/or Ala-Laurila.

CONCLUSION

As shown by the above analysis, the claimed subject matter is not anticipated or rendered obvious by the applied references. The prior art rejection should be withdrawn, and the pending claims allowed.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Hyung N. Sohn
Reg. No. 44,346

HNS/edg
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100